UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/739,260	12/19/2000	Ravi Sandhu	3001-07	5789

20457 7590 07/09/2004

ANTONELLI, TERRY, STOUT & KRAUS, LLP
1300 NORTH SEVENTEENTH STREET
SUITE 1800
ARLINGTON, VA 22209-9889

EXAMINER	
DAVIS, ZACHARY A	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 07/09/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/739,260	SANDHU ET AL.	
	Examiner	Art Unit	
	Zachary A Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 December 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *02 May 2001* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *6, 7*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Drawings

1. The drawings are objected to because many of the labels are handwritten and difficult to read. A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Information Disclosure Statement

2. US Patent 6005939, to Fortenberry, et al, was received with the Information Disclosure Statement received 07 June 2002 but was not cited on the accompanying Form PTO-1449. It has been considered by the Examiner and has been cited on the Form PTO-892 accompanying this Office action.

Claim Objections

3. Claim 14 is objected to because of the following informalities:

Claim 14 reads "A system according to claim 31" in line 1; however, it appears that the claim is instead intended to depend from Claim 13.

Appropriate correction is required.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 17 and 26 are rejected under 35 U.S.C. 102(b) as being anticipated by Ganesan, US Patent 5535276.

In reference to Claim 17, Ganesan discloses a system including a first networked device representing a user that generates a first private key portion, transforms a message with the first portion to form a second message (where the second message is the first encrypted message formed at column 8, lines 24-27; see also column 15, lines 52-54), and transmits the second message (column 8, lines 24-32). Ganesan also discloses a second networked device that stores a public key and a second private key portion (column 14, lines 59-66), receives the second message (column 8, lines 24-32), and further transforms the second message with the second private portion (column 8, lines 28-32; see also column 15, lines 61-63).

In reference to Claim 26, Ganesan discloses a method including generating a first private key portion, transforming a message with the first portion (column 8, lines 24-27), and further transforming the first message with the second private key portion (column 8, lines 28-32).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1-16, 18-25, and 27-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ganesan, US Patent 5535276, in view of Spies et al, US Patent 6230269.

In reference to Claim 1, Ganesan discloses a system including a first processor that generates a private key and public key pair (column 14, lines 29-30); divides the private key into a first portion, which is a user's password, and a second portion (column 14, lines 30-34); destroys the private key and the first portion (column 14, line 66-column 15, line 2); and stores the second portion and the public key (column 14, lines 59-66). Ganesan also discloses a second processor representing the user that generates the first private key portion upon input of the user's password (column 14, lines 30-32) and then destroys the first portion (column 14, line 66-column 15, line 2; column 19, lines 27-29). However, although Ganesan discloses that the first private key portion is a user's password, Ganesan does not explicitly disclose that the first portion is generated based on the user's password.

Spies discloses an authentication system in which a key is formed from a user's password (column 7, lines 36-41).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Ganesan by generating the first private key portion based on the user's password, instead of using the password itself as the first portion, in order to allow users the increased flexibility and convenience of generating keys at any computer on a network using only a password (see Spies, column 2, lines 45-48).

In reference to Claim 2, Ganesan further discloses that the user password has a bit length between 56 and 72 bits (column 8, lines 16-17; also column 3, lines 31-40).

In reference to Claim 3, Spies further discloses generating the first portion using a one way function (column 5, lines 35-37; column 7, lines 36-41).

In reference to Claim 4, Spies further discloses that the processors can operate in two modes (column 7, lines 36-47; column 8, lines 17-24) and that the one way function can be applied a varying number of times (column 5, lines 35-37).

In reference to Claims 5 and 7, Spies further discloses relying on the strength of the user password in generating keys (column 8, lines 19-21).

In reference to Claim 6, Spies further discloses selecting the one way function from a group of one way functions (column 5, lines 42-46).

In reference to Claim 8, Ganesan further discloses that the second processor encrypts a message with the first private key portion (column 8, lines 24-27) and that

the first processor recovers the message using the second private key portion and the public key (column 8, lines 28-32).

In reference to Claim 9, Ganesan discloses a system including a first processor representing a user that generates a first private key portion, which is a user's password (column 14, lines 30-32); transforms a message using the first portion (column 8, lines 24-27); and destroys the first portion (column 14, line 66-column 15, line 2; column 19, lines 27-29). Ganesan also discloses a second processor that further transforms the transformed message by applying a second private key portion and a public key corresponding to the first portion (column 8, lines 28-32). However, although Ganesan discloses that the first private key portion is a user's password, Ganesan does not explicitly disclose that the first portion is generated based on the user's password.

Spies discloses an authentication system in which a key is formed from a user's password (column 7, lines 36-41).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Ganesan by generating the first private key portion based on the user's password, instead of using the password itself as the first portion, in order to allow users the increased flexibility and convenience of generating keys at any computer on a network using only a password (see Spies, column 2, lines 45-48).

In reference to Claim 10, Ganesan further discloses a storage device storing the second portion and the public key, that the second processor retrieves the stored

second portion and public key, and that the first portion is never stored in a persistent state (column 14, line 59-column 15, line 2).

In reference to Claim 11, Ganesan further discloses that the user password has a bit length between 56 and 72 bits (column 8, lines 16-17; also column 3, lines 31-40).

In reference to Claim 12, Spies further discloses generating the first portion using a one way function (column 5, lines 35-37; column 7, lines 36-41).

In reference to Claim 13, Spies further discloses that the processors can operate in two modes (column 7, lines 36-47; column 8, lines 17-24) and that the one way function can be applied a varying number of times (column 5, lines 35-37).

In reference to Claims 14 and 16, Spies further discloses relying on the strength of the user password in generating keys (column 8, lines 19-21).

In reference to Claim 15, Spies further discloses selecting the one way function from a group of one way functions (column 5, lines 42-46).

In reference to Claim 18, Ganesan discloses a method including generating a private key and a public key (column 14, lines 29-30), dividing the private key into a first portion and a second portion (column 14, lines 30-34), destroying the private key and the first portion without storage (column 14, line 66-column 15, line 2), generating the first portion (column 14, lines 30-32), and destroying the first portion without storage (column 14, line 66-column 15, line 2; column 19, lines 27-29). However, although Ganesan discloses that the first private key portion is a user's password, Ganesan does

not explicitly disclose that the private key and the first portion are generated based on the user's password.

Spies discloses an authentication system in which a key is formed from a user's password (column 7, lines 36-41).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Ganesan by generating the first private key portion based on the user's password, instead of using the password itself as the first portion, in order to allow users the increased flexibility and convenience of generating keys at any computer on a network using only a password (see Spies, column 2, lines 45-48).

In reference to Claim 19, Ganesan further discloses that the user password has a bit length between 56 and 72 bits (column 8, lines 16-17; also column 3, lines 31-40).

In reference to Claim 20, Spies further discloses generating the first portion using a one way function (column 5, lines 35-37; column 7, lines 36-41).

In reference to Claim 21, Spies further discloses that the processors can operate in two modes (column 7, lines 36-47; column 8, lines 17-24) and that the one way function can be applied a varying number of times (column 5, lines 35-37).

In reference to Claim 22, Spies further discloses relying on the strength of the user password in generating keys (column 8, lines 19-21).

In reference to Claim 23, Spies further discloses selecting the one way function from a group of one way functions (column 5, lines 42-46) and relying on the strength of the user password in generating keys (column 8, lines 19-21).

In reference to Claim 24, Ganesan further discloses transforming a message with the first portion (column 8, lines 24-27) and further transforming the message using the second portion and the public key (column 8, lines 28-32).

In reference to Claim 25, Ganesan further discloses storing and retrieving the second portion and the public key and that the first portion is never stored in a persistent state (column 14, line 59-column 15, line 2).

In reference to Claim 27, Ganesan discloses everything as applied to Claim 26 above. Ganesan further discloses that the first private key portion is a password (column 14, lines 30-32) having a bit length of 56 to 72 bits (column 8, lines 16-17, and column 3, lines 31-40). However, although Ganesan discloses that the first private key portion is a user's password, Ganesan does not explicitly disclose that the first portion is generated based on the user's password.

Spies discloses an authentication system in which a key is formed from a user's password (column 7, lines 36-41).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Ganesan by generating the first private key portion based on the user's password, instead of using the password itself as the first portion, in order to allow users the increased flexibility and convenience of generating keys at any computer on a network using only a password (see Spies, column 2, lines 45-48).

In reference to Claim 28, Spies further discloses generating the first portion using a one way function (column 5, lines 35-37; column 7, lines 36-41).

In reference to Claim 29, Spies further discloses that the processors can operate in two modes (column 7, lines 36-47; column 8, lines 17-24) and that the one way function can be applied a varying number of times (column 5, lines 35-37).

In reference to Claim 30, Spies further discloses relying on the strength of the user password in generating keys (column 8, lines 19-21).

In reference to Claim 31, Spies further discloses selecting the one way function from a group of one way functions (column 5, lines 42-46) and relying on the strength of the user password in generating keys (column 8, lines 19-21).

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Lipner et al, US Patent 5210795, discloses a secure authentication method including forming a key as a "slow hash" of a user's password.

b. Kaufman et al, US Patent 5428854, discloses a system for protecting confidentiality of passwords including transforming a password into a key using a hash function.

c. Perlman, US Patent 5892828, discloses a system using a single password verification in which a hash of a password is created, after which the password itself is deleted.

d. Angelo et al, US Patent 5953422, discloses an authentication system using a network password, which is an encrypted or hashed version of a user password. Angelo also discloses using a split key system.

e. Eldridge et al, US Patent 6094721, discloses a method for password-based authentication in which a key may be formed from a password or from a hash function of a password.

f. Cuccia et al, US Patent 6151676, discloses a public key cryptosystem in which a passphrase is hashed to produce a key.

g. Stein, US Patent 6370250, discloses a method of authentication including a key formed from a hash of a password, and further discloses the use of password strength rules and strong hash functions for increased security.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A Davis whose telephone number is (703) 305-8902. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ZAD
zad

Matthew D. Smithers
MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137